REMARKS

In the Official Action mailed on **09 June 2008**, the Examiner reviewed claims 1-6, 9-20, and 23-25. Examiner rejected claims 1, 2, 13, 16, and 17 under 35 U.S.C. § 103(a) based on Hermann, Reto (EPO Publication No. EP1024626A1, hereinafter "Hermann") and Walker (U.S. Pub. No. 2003/0093663, hereinafter "Walker"). Examiner rejected claims 3-6, 12, 14, 18-20, and 25 under 35 U.S.C. § 103(a) based on Hermann, Walker, and Harrisville-Wolff et al. (U.S. Pub. No. 2004/0030887, hereinafter "Harrisville-Wolff"). Examiner rejected claims 9, and 15 under 35 U.S.C. § 103(a) based on Hermann, Walker, and Thompson et al. (U.S. Pub. No. 2002/0022483, hereinafter "Thompson"). Examiner rejected claims 10-11, 23, and 24 under 35 U.S.C. § 103(a) based on Hermann, Walker, and Thompson and Harrisville-Wolff et al. (U.S. Pub. No. 2004/0030887, hereinafter "Harrisville-Wolff").

Rejections under 35 U.S.C. § 103(a))

Claims 1, 2, 7, 8, 13, 16, and 17 were rejected under 35 U.S.C. § 103(a) based on Hermann, and further on Walker. Applicant respectfully disagrees.

Specifically, Applicant points out that the pre-authentication used by embodiments of the present invention involves the following steps (see paragraphs [0068]-[0071] of the instant application):

(1) exchanging key commitment information between the provisioning device and the network device over the bidirectional preferred channel;

(2) exchanging keys between the provisioning device and the network device over a bidirectional channel which does not have to be the preferred channel; and

(3) verifying the received keys using the received key commitment information on both the provisioning device and the network device.

Note that the above pre-authentication process is different from the authenticating session disclosed by Hermann in at least the following aspects.

First, the pre-authentication process of embodiments of the present invention involves separately exchanging authentication information by first exchanging key commitment information; and then exchanging keys. Note that these two exchanges are separate because they do not have to occur on the same communication channel (see paragraph [0070], lines 4-5 of the instant application). Also note that the above exchanges are bidirectional and hence are made over the respective **bidirectional communication channel(s).** In contrast, the authentication session of Hermann involves passing via **a unidirectional communication channel**, a sequence or an initial-sequence of authentication related information from the personal device to the serving device (see Hermann, paragraph [0021], line 5). Furthermore, Hermann did not disclose passing the key commitment information separately from passing the keys (see Hermann, paragraph [0021]).

Secondly, the pre-authentication process of the present invention involves using the received key commitment information to verify the received keys **on both the provisioning device and the network device without sending encrypted information back to each other**. In contrast, Hermann performs authentication by sending back encrypted information from the serving device to the personal device. Note that this step also involves a number of differences. First, embodiments of the present invention perform authentication (i.e., verifying the keys) on each of the provisioning device and the network device without having to return the encrypted information. This is possible because each device receives both key commitment information and keys, and hence can perform the key verification using the received information on the receiving device(s). Secondly, the present invention uses the key commitment information to verify the keys. In contrast, Hermann is silent on how the keys are authenticated.

There is nothing, either explicit or implicit, in the combined system of Hermann and Walker that discloses that pre-authenticating the network device involves: (1) exchanging key commitment information between the provisioning device and the network device over the bidirectional preferred channel; (2) exchanging keys between the provisioning device and the network device over a bidirectional channel which does not have to be the preferred channel; and (3) verifying the received keys using the received key commitment information on both the provisioning device and the network device.

Accordingly, Applicant has amended independent claims 1, 13, and 16 to clarify that the present invention provides a technique for pre-authenticating the network device by: (1) **exchanging key commitment** information between the provisioning device and the network device **over the bidirectional preferred channel** ; (2) **exchanging keys** between the provisioning device and the network device **over a bidirectional channel which does not have to be the preferred channel**; and (3) verifying the received keys using the received key commitment information on both the provisioning device and the network device. These amendments find support in paragraphs [0068]-[0071] of the instant application. No new matter has been added.

Hence, Applicant respectfully submits that independent claims 1, 13, and 16 as presently amended are in condition for allowance. Applicant also submits that claims 2-6 and 9-12 which depend upon claim 1, claims 14-15, which depend upon claim 13, and claims 17-20 and 23-25, which depend upon claim 16, are for the same reasons in condition for allowance and for reasons of the unique combinations recited in such claims.

CONCLUSION

It is submitted that the present application is presently in form for allowance. Such action is respectfully requested.

Respectfully submitted,

By /Shun Yao/_____
Shun Yao
Registration No. 59,242

Date: 9 October 2008

Shun Yao
Park, Vaughan & Fleming LLP
2820 Fifth Street
Davis, CA 95618-7759
Tel: (530) 759-1667
Fax: (530) 759-1665
Email: shun@parklegal.com